REMARKS

Applicants wish to thank the Examiner for his telephonic discussion regarding the subject case April 14, 2008. Applicants have amended the claims to better clarify aspects of the present invention.

In the Office Action mailed October 15, 2007, the Examiner rejected Claims 1-6, 15, 16, 19, 20 and 52-57 under 35 U.S.C.102(e) in view of Colosso (U.S. Patent 6,169, 976). In view of the claims as amended, Applicants respectfully submit that the rejection fails to establish the prima facie case of anticipation as each and every element of claims 1-6, 15, 16, 19, 20 and 52-57 are not taught or suggested by Colosso. New claims 59-67 are not only allowable independently but also by virtue of their dependence on allowable independent Claim 1.

Specifically, Colosso does not teach or suggest a method that operates by,

" receiving a request for an access permission security profile on behalf of a network user that gives the network user the ability to access one or more objects associated with a domain according to the network user's membership in one or more groups within the domain;",
"authenticating the request from the network user according to an n-factor authentication suitable to the plurality of network users and verifying membership in the domain and the one or more groups",

"creating the access permission security profile having an ephemeral crytpographic characterstic and derived from a combination of the user's membership in the one or more groups, wherein the combination of the user's membership in the one or more groups can be used to form a cryptographic key for enabling the network user to decrypt selected portions of an encrypted object when one or more groups associated with the encrypted object match the network user's membership in one or more groups within the domain and to encrypt selected portions of a plaintext object to be accessed by other network user's when the other network user's membership in one or more groups within the domain also match the one or more groups associated with the selected portions of the plaintext object being encrypted;" and

"securely transmitting the access permission security profile to the network user over the network wherein the ephemeral cryptographic characteristic allows the network user in receipt of the access permission security profile to perform cryptogrpahic operations for a predetermined period of time" as recited in claim 1.

Dependent claims 2-3, 16-22, and 57-67 are not only in condition for allowance independently but also by virtue of their dependence on allowable independent claim 1.

Claim 4 as amended also is in condition for allowance. In particular, Colosso does not teach or suggest, "receiving a request for decryption capabilities on behalf of a network user that gives the network user the ability to decrypt one or more encrypted objects associated with a domain according to the network user's membership in one or more groups within the domain",

"authenticating the request from the network user according to an n-factor authentication suitable to the plurality of network users and verifying that they are members of the domain and the one or more groups;"

"creating an access permission security profile derived from a combination of the user's membership in the one or more groups, wherein the combination of the user's membership in the one or more groups can be used to form a cryptographic key and decrypt selected portions of the one or more encrypted objects ;"

"receiving information associated with the selected portions of an encrypted object;"

" generating a cryptographic working key using the cryptographic key from the access permission security profile and the received information associated with the selected portions of the encrypted object;" and

" securely transmitting the cryptographic working key to the network user over the network allowing the network user to decrypt other than the selected portions of the encrypted object" as recited in Claim 4.

Further, Claims 5 and 6 are in condition for allowance both independently and by virtue of their dependence on allowable Claim 4.

Claims 15-22 are not only allowable independently but also by virtue of their dependence on allowable Claims 1, 4 and 7.

Colosso also does not disclose or suggest a centralized security management system for distributing cryptographic capabilities to a plurality of network users over a decentralized public network" as recited in Claim 52. Specifically, Colosso does not disclose or suggest "a set of client systems, wherein each client system includes means for receiving the requested member token and means for utilizing the cryptographic capabilities provided by the member token for selective encryption and decryption." As previously described, Colosso is concerned about authenticating the customer as a valid licensee at a web-based system and then using a key to authenticate the same customer to the licensed software they have licensed for a fee. (Column 8, line 55 to Column 9, line 39; and Column 12, line 65 to Column 15, line 25). There is no mention of both encrypting the licensed software and decrypting the licensed software since the customer is interested in only activating the software to execute certain functions.

For at least this reason, Claim 52 also remains in condition for allowance. Claims 53-58 also are independently allowable as well as allowable by virtue of their dependence on allowable Claim 52.

For at least these reasons above, the Applicants would respectfully request the Examiner to withdraw the rejection of Claims 1-6, 15, 16, 19, 20 and 52-57 under 35 U.S.C.102(e) in view of Colosso.

In addition, the Examiner rejected claims 7-11, 13-16, 19, 20, and 57 under 35 USC 103(a) over Colosso in view of Shanton (U.S. Patent 5,680,452).

Applicants respectfully submit that combining Colosso with Shanton does not teach or suggest each and every limitation of Claim 7. In particular, Colosso in view of Shanton does not teach or suggest,

"creating a computer representable data object including one or more embedded objects;",

"associating a pseudorandom cryptographic key with each of the one or more embedded objects of the data object to be encrypted;",

"encrypting each of the embedded objects using a working key derived from the respective pseudorandom cryptographic key associated with the embedded object and other components;"

"creating a set of one or more access permission credentials that identify the roles each of the plurality of network users may possess in a domain and their membership in one or more groups as defined by various combinations of the one or more access permission credentials;"

"assigning a member credential to each of the selected embedded objects, wherein the member credential is a specific combination of the one or more access permission credentials ensuring that only network users having a matching member credential are able to decrypt encrypted embedded objects of the data object;"

"inserting the pseudorandom cryptographic key in the header of each embedded object after first encrypting the pseudorandom cryptographic key with a credential key derived from the member credential associated with each embedded object;"

"transmitting the data object over the network having the encrypted pseudorandom key inserted in a portion of the embedded object;" and

"securely transmitting an access permission security profile, having an ephemeral crytpographic characterstic, to at least one network user from the plurality of network users wherein the access permission security profile for the at least one network user can be used to generate a credential key capable of decrypting the encrypted pseudorandom cryptographic key associated with the encrypted object because the member credential of the network user matches the member credentials associated with the encrypted object, wherein the ephemeral cryptographic characteristic allows the network user in receipt of the access permission security profile to perform cryptogrpahic operations for a predetermined period of time." as recited in Claim 7.

For one or more of the aforementioned reasons, Claim 7 as amended is in condition for allowance. Claims 8-14 and Claims 15-33 and 57 also remain in condition for allowance independently as well as directly or indirectly through their dependence on allowable independent Claim 7.

Accordingly, the Applicants respectfully requests that the Examiner withdraw the rejection of claims 7-11, 13-16, 19, 20, and 57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Colosso in view of Shanton.

Applicants also respectfully request that the Examiner withdraw the rejection of Claims 17, 18 and 58 under 35 U.S.C. 103(a) as being unpatentable over Colosso in view of Kennedy and unpatentable over Colloso in view of Shanton and further in view of Kennedy. Claims 17, 18 and 58 are at allowable by virtue of their dependence on allowable independent Claim 1.

With respect to Claims 21 and 22, these claims at least depend on allowable independent Claim 1. Applicants also request withdrawal of the rejection of Claims 21 and 22 under 35 U.S.C. 103(a) over Colosso in view of Win and over Colosso in view of Shanton and further in view of Win.

Claims 1-16, 18-22, 52, and 54-57 are rejected under 35 U.S.C. 103(a) over Halter (U.S. Patent 5,319,705) in view of Win (U.S. Patent 6,161,139).

Applicant respectfully submits that Halter in view of Win do not teach or suggest

" receiving a request for an access permission security profile on behalf of a network user that gives the network user the ability to access one or more objects associated with a domain according to the network user's membership in one or more groups within the domain;",

"authenticating the request from the network user according to an n-factor authentication suitable to the plurality of network users and verifying membership in the domain and the one or more groups",

"creating the access permission security profile having an ephemeral crytpographic characterstic and derived from a combination of the user's membership in the one or more groups, wherein the combination of the user's membership in the one or more groups can be used to form a cryptographic key for enabling the network user to decrypt selected portions of an encrypted object when one or more groups associated with the encrypted object match the network user's membership in one or more groups within the domain and to encrypt selected portions of a plaintext object to be accessed by other network user's when the other network user's membership in one or more groups within the domain also match the one or more groups associated with the selected portions of the plaintext object being encrypted;" and

"securely transmitting the access permission security profile to the network user over the network wherein the ephemeral cryptographic characteristic allows the network user in receipt of the access permission security profile to perform cryptogrpahic operations for a predetermined period of time" as recited in claim 1.

In particular, Halter in view of Win does not teach or suggest that :

"creating the access permission security profile having an ephemeral crytpographic characterstic and derived from a combination of the user's membership in the one or more groups, wherein the combination of the user's membership in the one or more groups can be used to form a cryptographic key for enabling the network user to decrypt selected portions of an encrypted object

when one or more groups associated with the encrypted object match the network user's membership in one or more groups within the domain and to encrypt selected portions of a plaintext object to be accessed by other network user's when the other network user's membership in one or more groups within the domain also match the one or more groups associated with the selected portions of the plaintext object being encrypted" and also that

"the ephemeral cryptographic characteristic allows the network user in receipt of the access permission security profile to perform cryptogrpahic operations for a predetermined period of time" in addition to the other limitations provided above in Claim 1.

For at least this additional reason Claim 1 remains patentable over Haller in view of Win. Claims 4, 7 and 52 are allowable for at least the same or similar reasons as are dependent claims 2-3, 5-6, 8-14, 15-22, and 53-58 which depend directly or indirectly from one or more of the aforementioned allowable independent claims.

In summary, Applicants respectfully request reconsideration and withdrawal of the rejections and allowance of the claims as amended.

///

///

///

///

///

///

///

///

///

///

///

///

///

///

The Applicant has made a diligent effort to place the claims in condition for allowance, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Leland Wiesner, Applicants' Attorney at (650) 853-1113 so that such issues may be resolved as expeditiously as possible.

Applicant	:	Sweet et al.
Atty Dkt.	:	00131-000100000
Issued	:	n/a
Serial No.	:	09/930,029
Filed	:	08/14/2001
Page	:	Page 26 of 26

For these reasons provided above, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Respectfully Submitted,

April 15, 2008
Date

Leland Wiesner
Attorney/Agent for Applicant(s)
Reg. No. 39424

Wiesner and Associates
366 Cambridge Ave.
Palo Alto, California 94306
Tel. (650) 853-1113